We claim:

1. A computerized system for monitoring application usage, the method comprising:

receiving transaction activity from at least one of the group consisting of: transaction activity related to the use of a computer application by a user, firewall activity, network operating system activity, and operating system activity;

parsing the transaction activity;

building a profile for the user based on the parsed transaction activity.

2. A computerized method for monitoring application usage, the method comprising

receiving transaction activity from at least one of the group consisting of: transaction activity related to the use of a computer application by a user, firewall activity, network operating system activity, and operating system activity;

parsing the transaction activity

comparing a subset of the parsed transaction activity associated with a user to a predetermined profile for the user, said profile based at least in part on earlier transaction activity of the user;

generating an alert if any of the parsed transaction activity is not consistent the predetermined profile.

3. The method of claim 2, wherein the computer application includes computer applications selected from the group consisting of PeopleSoft, SAP, and JD Edwards.

4. The method of claim 2, wherein the transaction activity further includes transaction activity from an access and authentication system; and further comprising generating a set of forensic data based on the transaction activity.

5. The method of claim 2, wherein the transaction activity is sent to a remote system prior to parsing the transaction activity.

6. The method of claim 5, wherein the transaction activity is encrypted prior to sending to the remote system.

7. The method of claim 2, wherein the profile includes working hours for the user.

8. The method of claim 7, wherein the a time a transaction is executed by the user is determined by the transaction activity and is utilized to determine if the transaction was performed during the authorized working hours for the user.

9. The method of claim 7, wherein the working hours are set by a system administrator.

10. The method of claim 2, wherein the profile includes transaction normally executed by the user.

11. The method of claim 2, wherein generating an alert includes generating an alert if more than one transaction has been executed by a single user during substantially the same period or overlapping periods of time.

12. The method of claim 2, wherein generating an alert includes generating an alert if more than one network logon has been executed by a single user during substantially the same period or overlapping periods of time.

13. The method of claim 2, wherein generating an alert includes generating an alert if a transaction is executed by a user from a device that is other than that assigned to the user.

14. The method of claim 2, further comprising generating an alert if a transaction is executed by an un-identified user.

15. The method of claim 2, further comprising generating an alert if a transaction is executed by a user that is not known to the application.

16. The method of claim 2, further comprising generating an alert if a transaction is executed by a user that has been terminated.

17. The method of claim 2, further comprising generating a billing record based on the transaction activity.

18. The method of claim 17, wherein the billing record is generated based on the volume of transaction activity.

19. The method of claim 17, wherein the billing record is generated based on a number of transactions in the transaction activity.

20. A computerized system for monitoring computer application use comprising:

a transaction activity harvester operable to receive transactions, said transaction including transactions received from the group consisting of: a computer application, firewall, network operating system, and operating system;

a transaction parser operable to parse the transactions;

an analytical profile builder operable to create a profile for a user, said profile comprising a set of valid transactions for the user;

a monitoring and alert system operable to compare a transaction executed by the user in the computer application with the set of valid transactions for the user and to generate an alert if the executed transaction is not consistent with the set of valid transactions.

21. The system of claim 20, wherein the monitoring and alert system is further operable to generate an alert upon detecting repeated attempts to access secured transactions by a user.

22. The system of claim 20, wherein the set of valid transactions includes transactions the user has executed in the past.

23. The system of claim 20, wherein an alert is generated if more than one transaction has been executed by a single user during substantially the same period or overlapping periods of time.

24. The system of claim 20, wherein an alert is generated if a transaction is executed by a user from a device that is other than that assigned to the user.

25. The system of claim 20, wherein an alert is generated if a transactions is executed by the user outside of the standard work days and hours for the user.

26. The system of claim 20, wherein an alert is generated if a transaction is executed by an un-identified user.

27. The system of claim 20, wherein an alert is generated if a transaction is executed by a user that is not known to the application.

28. The system of claim 20, further comprising a client identification builder operable to identify a set of users to be monitored.

29. The system of claim 20, further comprising a transaction identification builder operable to identify a set of transactions to be monitored.

30. The system of claim 20, wherein the transaction activity harvester is further operable to receive transaction activity from an operating system.

31. The system of claim 20, further comprising a firewall and wherein the transaction activity harvester is further operable to receive transaction activity from the firewall.

32. The system of claim 20, further comprising a network operating system and wherein the transaction activity harvester is further operable to receive transaction activity from the network operating system.

33. The system of claim 20, further comprising a rules engine operably coupled to a rules database containing a set of rules to be applied by the monitoring and alert system.